



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/017,988	12/06/2001	Ronald C. Card	80398P490	8402

8791 7590 06/10/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN  
12400 WILSHIRE BOULEVARD  
SEVENTH FLOOR  
LOS ANGELES, CA 90025-1030

EXAMINER

TESLOVICH, TAMARA

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 06/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>		<b>Applicant(s)</b>	
	10/017,988		CARD, RONALD C.	
	<b>Examiner</b>		<b>Art Unit</b>	
	Tamara Teslovich		2137	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 06 December 2001.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-48 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-48 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 December 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)               | Paper No(s)/Mail Date. _____  |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>02.26.02 03.07.02</u> <u>11.01.02</u> <u>07.16.03</u>                     | 6) <input type="checkbox"/> Other: _____                                    |
| <u>06.04.04</u> <u>05.18.04</u> <u>03.25.04</u> <u>10.14.03</u>                                    |   |
| <u>08.05.04</u> <u>10.14.04</u> <u>12.16.04</u>  |   |

**DETAILED ACTION**

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

5 form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

10 (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

15 **Claims 1-48 are rejected under 35 U.S.C. 102(e) as being anticipated by Wheeler et al., U.S. Patent Application Publication No. 2003/0126439 A1.**

As per claim 1, Wheeler discloses a method comprising: transmitting  
identification information related to a user to an authentication entity (access  
20 authentication component); and receiving access to a secure entity (controlled  
resource) coupled to said authentication entity (access authentication component) if  
authentication information identifying said user is provided to said secure entity  
(controlled resource) ([0061]).

25 As per claim 2, Wheeler discloses the method according to claim 1, wherein said  
transmitting further comprises: transmitting at least one access question to said  
authentication entity (access authentication component), said at least one access

question being tailored by said user based on said identification information in order to uniquely identify and authenticate said user ([0061]).

As per claim 3, Wheeler discloses the method according to claim 1, wherein said  
5 authentication information includes a level of authentication related to a location of said user when requesting said access information is based on a profile of said user stored in said authentication entity (access authentication component) ([0130]).

As per claim 4, Wheeler discloses the method according to claim 1, wherein said  
10 authentication information is based on a profile of said user stored in said authentication entity (access authentication component) ([0087]).

As per claim 5, Wheeler discloses the method according to claim 4, wherein said  
profile contains said identification information related to said user and at least one level  
15 of authentication related to a location of said user when requesting said access ([0130]).

As per claim 6, Wheeler discloses the method according to claim 2, wherein said  
receiving further comprises: receiving an authentication request from said secure entity  
(controlled component); transmitting said authentication request to said authentication  
20 entity (access authentication component); receiving said at least one access question  
(secret) from said authentication entity (access authentication component); and

transmitting an answer to said at least one access question to said authentication entity (access authentication component) to authenticate said user ([0063],[0065]; Figure 14).

As per claim 7, Wheeler discloses the method according to claim 2, wherein said  
5 receiving further comprises: receiving said at least one access question from said authentication entity (access authentication component); and transmitting an answer to said at least one access question to said authentication entity (access authentication component) to authenticate said user ([0061]).

10 As per claim 8, Wheeler discloses the method according to claim 2, wherein said transmitting further comprises establishing biometric access (such as fingerprint recognition) to said authentication entity (access authentication component) using a biometric control module (biometric input pad) ([0013],[0133]).

15 As per claim 9, Wheeler discloses the method according to claim 1, wherein said receiving further comprises: receiving at least one access question from said authentication entity (access authentication component), said at least one access question being created by said authentication entity (access authentication component) based on said identification information in order to uniquely identify and authenticate  
20 said user; and providing an answer to said at least one access question (secret) to said authentication entity (access authentication component) to authenticate said user ([0061]).

As per claim 10, Wheeler discloses the method according to claim 1, wherein said secure entity specifies a plurality of authenticated users (employees) to said authentication entity (access authentication component) and said authentication entity  
5 stores, said authentication information related to each authenticated user of said plurality of authenticated users ([0076]).

As per claim 11, Wheeler discloses the method according to claim 1, wherein said authentication entity is a transaction privacy clearing house (TPCH) server (a  
10 system maintaining secure accounts on behalf of requesting account holders) ([0051]).

As per claim 12, Wheeler discloses a method comprising: receiving an authentication request related to a user requesting access to a secure entity; retrieving a profile of said user from an access database, said profile containing at least one  
15 access question uniquely identifying said user; and transmitting authentication information to said secure entity based on an answer to said at least one access question (secret) received from said user ([0012-0013],[0065],[0087]; Figure 14)

As per claim 13, Wheeler discloses the method according to claim 12, wherein  
20 said authentication request is received directly from said secure entity (system) ([0063]).

As per claim 14, Wheeler discloses the method according to claim 12, wherein said authentication request is received from a personal transaction device coupled to said user and to said secure entity ([0020]).

5 As per claim 15, Wheeler discloses the method according to claim 12, wherein said authentication information is transmitted directly to said secure entity ([0019]).

As per claim 16, Wheeler discloses the method according to claim 12, wherein said authentication information is transmitted to a personal transaction device coupled  
10 to said user and to said secure entity ([0020]).

As per claim 17, Wheeler discloses the method according to claim 12, further comprising:

receiving identification information related to said user from a personal  
15 transaction device coupled to said user and said secure entity, said identification information including said at least one access question (secret); and ([0012-0013])

storing said at least one access question and at least one level of authentication in said profile within said access database, said at least one level of authentication being related to a location of said user when requesting said access ([0021-0022],  
20 [0058], [0130]).

As per claim 18, Wheeler discloses the method according to claim 17, wherein said personal transaction device establishes biometric access to transmit said identification information using a biometric control module ([0012-0013], [0133]).

5 As per claim 19, Wheeler discloses the method according to claim 12, wherein said authentication information includes a level of authentication related to a location of said user when requesting said access ([0130]).

As per claim 20, Wheeler discloses the method according to claim 12, further  
10 comprising:

receiving identification information related to said user from a personal transaction device coupled to said user and said secure entity ([0020-21]);

creating said at least one access question based on said identification information; and storing said at least one access question and at least one level of  
15 authentication in said profile within said access database, said at least one level of authentication being related to a location of said user when requesting said access ([0012-0013], [0058], [0130]).

Claims 21-26 are directed towards a system's implementation of the method of  
20 claims 12-17 and are rejected by similar rationale.



Claims 27-28 are directed towards a system's implementation of the method of claims 19-20 and are rejected by similar rationale.

Claim 29 is directed towards a system's implementation of the method of claim  
5 18 and is rejected by a similar rationale.

As per claim 30, Wheeler discloses the system according to claim 21, wherein said personal transaction device receives said at least one access question from said authentication entity and transmits said answer to said authentication entity to  
10 authenticate said user ([0019]).

As per claim 31, Wheeler discloses an apparatus comprising: means for transmitting identification information related to a user to an authentication entity; and means for receiving access to a secure entity coupled to said authentication entity if  
15 authentication information identifying said user is provided to said secure entity ([0020],[0022]).

As per claim 32, Wheeler discloses the apparatus according to claim 31, further comprising: means for transmitting at least one access question (secret) to said  
20 authentication entity said at least one access question being tailored by said user based on said identification information in order to uniquely identify and authenticate said user ([0012-0013]).

As per claim 33, Wheeler discloses the apparatus according to claim 32, further comprising:

means for receiving an authentication request from said secure entity ([0063]);

5 means for transmitting said authentication request to said authentication entity ([0063]);

means for receiving said at least one access question from said authentication entity; and means for transmitting an answer to said at least one access question to said authentication entity to authenticate said user ([0061]).

10

As per claim 34, Wheeler discloses the apparatus according to claim 32, further comprising: means for receiving said at least one access question from said authentication entity; and means for transmitting an answer to said at least one access question to said authentication entity to authenticate said user ([0012-0013]).

15

As per claim 35, Wheeler discloses the apparatus according to claim 32, further comprising: means for establishing biometric access to said authentication entity using a biometric control module ([0013], [0133]).

20

As per claim 36, Wheeler discloses the apparatus according to claim 31, further comprising: means for receiving at least one access question from said authentication entity, said at least one access question being created by said authentication entity

based on said identification information in order to uniquely identify and authenticate said user; and means for providing an answer to said at least one access question to said authentication entity to authenticate said user ([0012-0013]).

5           As per claim 37, Wheeler discloses an apparatus comprising: means for receiving an authentication request related to a user requesting access to a secure entity; means for retrieving a profile of said user from an access database, said profile containing at least one access question (secret) uniquely identifying said user; and means for transmitting authentication information to said secure entity based on an  
10 answer to said at least one access question received from said user ([0013], [0133], [0021]).

          As per claim 38, Wheeler discloses the apparatus according to claim 37, further comprising: means for receiving identification information related to said user from a  
15 personal transaction device coupled to said user and said secure entity, said identification information including said at least one access question (secret); and means for storing said at least one access question and at least one level of authentication in said profile within said access database said at least one level of authentication being related to a location of said user when requesting said access  
20 ([0013, 0133], [0130]).

As per claim 39, Wheeler discloses the apparatus according to claim 37, further comprising:

means for receiving identification information related to said user from a personal transaction device coupled to said user and said secure entity ([0019],[0021-0022]);

5 means for creating said at least one access question (secret) based on said identification information ([0013],[0015]); and

means for storing said at least one access question and at least one level of authentication in said profile within said access database, said at least one level of authentication being related to a location of said user when requesting said access  
10 ([0013,0133]).

Claims 40-45 are directed towards the apparatus of claims 31-36 wherein the apparatus is a computer-readable medium executing instructions within a processing system and are rejected by similar rationale.

15

Claims 46-48 are directed towards the apparatus of claims 37-39 wherein the apparatus is a computer-readable medium executing instructions within a processing system and are rejected by similar rationale.

20 **Claims 1-48 are rejected under 35 U.S.C. 102(e) as being anticipated by Maritzen et al., U.S. Patent Application Publication No. 2002/0026423 A1.**

As per claim 1, Maritzen discloses a method comprising:  
transmitting identification information related to a user to an authentication entity;  
and ([0033] lines 15-23; [0037])  
receiving access to a secure entity coupled to said authentication entity if  
5 authentication information identifying said user is provided to said secure entity ([0036]).

As per claim 2, Maritzen discloses the method according to claim 1, wherein said  
transmitting further comprises:  
transmitting at least one access question to said authentication entity, said at  
10 least one access question being tailored by said user based on said identification  
information in order to uniquely identify and authenticate said user ([0037] lines 15-20).

As per claim 3, Maritzen discloses the method according to claim 1, wherein said  
authentication information includes a level of authentication related to a location of said  
15 user when requesting said access information is based on a profile of said user stored  
in said authentication entity ([0059] lines 25-43).

As per claim 4, Maritzen discloses the method according to claim 1, wherein said  
authentication information is based on a profile of said user stored in said authentication  
20 entity ([0033] lines 15-23).

As per claim 5, Maritzen discloses the method according to claim 4, wherein said profile contains said identification information related to said user and at least one level of authentication related to a location of said user when requesting said access ([0037]).

5       As per claim 6, Maritzen discloses the method according to claim 2, wherein said receiving further comprises: receiving an authentication request from said secure entity; transmitting said authentication request to said authentication entity; receiving said at least one access question from said authentication entity; and transmitting an answer to said at least one access question to said authentication entity to authenticate said user  
10 ([0034, 0047]).

As per claim 7, Maritzen discloses the method according to claim 2, wherein said receiving further comprises: receiving said at least one access question from said authentication entity; and transmitting an answer to said at least one access question to  
15 said authentication entity to authenticate said user ([0033]).

As per claim 8, Maritzen discloses the method according to claim 2, wherein said transmitting further comprises establishing biometric access to said authentication entity using a biometric control module ([0032]).

20

As per claim 9, Maritzen discloses the method according to claim 1, wherein said receiving further comprises: receiving at least one access question from said

Art Unit: 2137

authentication entity, said at least one access question being created by said authentication entity based on said identification information in order to uniquely identify and authenticate said user; and providing an answer to said at least one access question to said authentication entity to authenticate said user ([0033-0034, 0047]).

5

As per claim 10, Maritzen discloses the method according to claim 1, wherein said secure entity specifies a plurality of authenticated users to said authentication entity and said authentication entity stores; said authentication information related to each authenticated user of said plurality of authenticated users ([0032]).

10

As per claim 11, Maritzen discloses the method according to claim 1, wherein said authentication entity is a transaction privacy clearing house (TPCH) server ([0033]).

15 As per claim 12, Maritzen discloses a method comprising: receiving an authentication request related to a user requesting access to a secure entity; retrieving a profile of said user from an access database, said profile containing at least one access question uniquely identifying said user; and transmitting authentication information to said secure entity based on an answer to said at least one access question received from said user ([0033]).

20

As per claim 13, Maritzen discloses the method according to claim 12, wherein said authentication request is received directly from said secure entity ([0034]).

As per claim 14, Maritzen discloses the method according to claim 12, wherein said authentication request is received from a personal transaction device coupled to said user and to said secure entity ([0032]).

5

As per claim 15, Maritzen discloses the method according to claim 12, wherein said authentication information is transmitted directly to said secure entity ([0034]).

As per claim 16, Maritzen discloses the method according to claim 12, wherein  
10 said authentication information is transmitted to a personal transaction device coupled to said user and to said secure entity ([0049]).

As per claim 17, Maritzen discloses the method according to claim 12, further comprising: receiving identification information related to said user from a personal  
15 transaction device coupled to said user and said secure entity, said identification information including said at least one access question; and storing said at least one access question and at least one level of authentication in said profile within said access database, said at least one level of authentication being related to a location of said user when requesting said access ([0033],[0054]).

20



As per claim 18, Maritzen discloses the method according to claim 17, wherein said personal transaction device establishes biometric access to transmit said identification information using a biometric control module ([0032]).

5 As per claim 19, Maritzen discloses the method according to claim 12, wherein said authentication information includes a level of authentication related to a location of said user when requesting said access ([0054]).

As per claim 20, Maritzen discloses the method according to claim 12, further  
10 comprising: receiving identification information related to said user from a personal transaction device coupled to said user and said secure entity; creating said at least one access question based on said identification information; and storing said at least one access question and at least one level of authentication in said profile within said access database, said at least one level of authentication being related to a location of  
15 said user when requesting said access ([0033],[0054]).

Claims 21-26 are directed towards a system's implementation of the method of claims 12-17 and are rejected by similar rationale.

20 Claims 27-28 are directed towards a system's implementation of the method of claims 19-20 and are rejected by similar rationale.

Claim 29 is directed towards a system's implementation of the method of claim 18 and is rejected by a similar rationale.

As per claim 30, Maritzen discloses the system according to claim 21, wherein  
5 said personal transaction device receives said at least one access question from said authentication entity and transmits said answer to said authentication entity to authenticate said user ([0033]).

As per claim 31, Maritzen discloses an apparatus comprising: means for  
10 transmitting identification information related to a user to an authentication entity (TCPH); and means for receiving access to a secure entity coupled to said authentication entity if authentication information identifying said user is provided to said secure entity ([0033]).

15 As per claim 32, Maritzen discloses the apparatus according to claim 31, further comprising: means for transmitting at least one access question to said authentication entity said at least one access question being tailored by said user based on said identification information in order to uniquely identify and authenticate said user ([0033]).

20

As per claim 33, Maritzen discloses the apparatus according to claim 32, further comprising: means for receiving an authentication request (confirmation that funds

exist) from said secure entity (financial processing unit) and means for transmitting said authentication request to said authentication entity (TCPH); means for receiving said at least one access question (request for user identification information) from said authentication entity (TCPH); and means for transmitting an answer to said at least one  
5 access question to said authentication entity to authenticate said user (transaction device providing user information to complete transactions) ([0034],[0037]).

As per claim 34, Maritzen discloses the apparatus according to claim 32, further comprising: means for receiving said at least one access question (request for  
10 information) from said authentication entity (TCPH); and means for transmitting an answer to said at least one access question to (fill in the blanks) said authentication entity to authenticate said user ([0033]).

As per claim 35, Maritzen discloses the apparatus according to claim 32, further  
15 comprising: means for establishing biometric access to said authentication entity using a biometric control module ([0032]).

As per claim 36, Maritzen discloses the apparatus according to claim 31, further comprising: means for receiving at least one access question from said authentication  
20 entity (TCPH), said at least one access question being created by said authentication entity based on said identification information in order to uniquely identify and

authenticate said user; and means for providing an answer to said at least one access question to said authentication entity to authenticate said user ([0033]).

As per claim 37, Maritzen discloses an apparatus comprising: means for  
5 receiving an authentication request related to a user requesting access to a secure entity (vendor/financial system); means for retrieving a profile of said user from an access database, said profile containing at least one access question uniquely identifying said user (i.e. mother's maiden name); and means for transmitting authentication information (account does exist, funds available) to said secure entity  
10 based on an answer to said at least one access question received from said user ([0033],[0036]).

As per claim 38, Maritzen discloses the apparatus according to claim 37, further comprising: means for receiving identification information related to said user from a  
15 personal transaction device coupled to said user and said secure entity, said identification information including said at least one access question; and means for storing said at least one access question and at least one level of authentication in said profile within said access database said at least one level of authentication being related to a location of said user when requesting said access ([0033],[0036],[0054]).

20

As per claim 39, Maritzen discloses the apparatus according to claim 37, further comprising: means for receiving identification information related to said user from a

personal transaction device coupled to said user and said secure entity; means for creating said at least one access question based on said identification information; and means for storing said at least one access question and at least one level of authentication in said profile within said access database, said at least one level of authentication being related to a location of said user when requesting said access ([0033],[0036],[0054]).

Claims 40-45 are directed towards the apparatus of claims 31-36 wherein the apparatus is a computer-readable medium executing instructions within a processing system and are rejected by similar rationale.

Claims 46-48 are directed towards the apparatus of claims 37-39 wherein the apparatus is a computer-readable medium executing instructions within a processing system and are rejected by similar rationale.

15

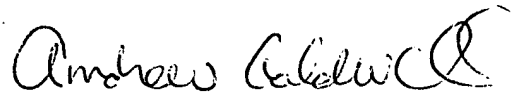
### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone

number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



**ANDREW CALDWELL**  
**SUPERVISORY PATENT EXAMINER**

May 18, 2005  
T.Teslovich